AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with the Apple ID and iCloud account grindfamily1@gmail.com that is stored at premises controlled by Apple Inc.

Case No. 19-968M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 USC 1951(a), 924(c), and 922(g)(1).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

ATF Special Agent Frank Rutter
Printed Name and Title

Sworn to before me and signed in my presence:

Date: November 21, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Frank Rutter, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the Apple ID and iCloud account grindfamily1@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been since 2015. As an ATF Agent, I have conducted firearms trafficking investigations involving violations of 18 U.S.C. § 922(a)(6), commonly referred to as "lying and buying" as well as investigations related to the unlawful use and possession of firearms by previously convicted felons in violation of 18 U.S.C. § 922(g)(1). Additionally I have conducted and participated in investigations involving violations of 18 U.S.C. § 924(c) (Use of a firearm in furtherance of crime of violence or drug trafficking crime). I have had a variety of formal, informal, and on the job training in the investigation of illegal firearms possession and trafficking. I have participated in the execution of search warrants in which firearms were seized; and I am familiar with the street name(s) of firearms and firearm related topics.

3. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law

enforcement officers, who have provided information to me during the course of their official duties and whom I consider to be truthful and reliable.

4. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, instrumentalities, and/or fruits of violations of Title 18, United States Code, Sections 1951(a) (Hobbs Act robbery), 924(c) (use of a firearm during a crime of violence), and Title 18, United States Code, Section 922(g)(1) (felon in possession of a firearm), as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On October 2, 2019, in the morning, an employee at the AT&T store located at 3543 South 27th Street, Milwaukee, Wisconsin, reported to the Milwaukee Police Department that at about 10:45 a.m. he had noticed a blue 4 door Hyundai Elantra backed in by a dumpster near the store. The car was occupied by two individuals who ducked down as he drove past them. Inside the store, the employee saw a black male approach the front door and attempt to open it. The employee stated that since a previous armed robbery on September 20, 2019, they keep the front door locked and only open it for customers. The subject then turned and walked away in the direction of the Hyundai. The employee left the store and drove thru the parking lot. He saw the

subject getting into the passenger door of the Hyundai. The employee took a photograph of the blue Hyundai with his cell phone as the car left the parking lot

8. Based upon the witness description and the recovered surveillance footage, the driver was a black male, wearing black clothing and weighing approximately 240 pounds. The passenger was a black male, early 30's, 5'8" to 5'9" tall, approximately 200 pounds, dark complexion, wearing a white baseball cap, zippered gray hooded sweatshirt with "Everlast" across the chest, bleached/distressed style blue jeans, black gloves, and a black sunglasses.

9. On October 2, 2019, at approximately 7:49 p.m., two masked subjects entered the Sprint store located at 4550 South 27th Street, Milwaukee, Wisconsin. Subject #1 demanded an employee go to the back room of the store. Subject #2, armed with a black handgun, threatened the victims that if they moved he would shoot them. Subject #1 told Subject #2 to have the other victims moved into the back room. The subjects demanded the employee open the safe where the cellular telephones were kept. Once the safe was open, the cellular phones were placed into black garbage bags. The subjects fled. Sprint was a business involved in interstate commerce at the time of the robbery.

10. Based upon witnesses' descriptions and the recovered surveillance footage, Subject #1 was a black male, approximately 30 years of age, approximately 5'7" tall, approximately 365 pounds, heavy build, wearing a black hooded sweatshirt, gray pants, black shoes, gloves, and a black face mask. Subject #2 was described as a black male, approximately 25 years of age, approximately 5'10" tall, approximately 170 pounds, medium build, wearing a zippered gray hooded sweatshirt with "Everlast" across the chest, bleached/distressed style blue jeans, gloves, and a black mask. The firearm, which was brandished during the robbery, was described as a black, semi-automatic handgun.

11. Law enforcement collected video from the Sprint store and conducted a canvas in the area, which resulted in several surveillance videos being recovered and reviewed. These videos captured the subjects exiting from and fleeing in a blue Hyundai Elantra.

12. On October 7, 2019, at approximately 12:18 p.m., an armed and masked subject entered the Sprint store located at 1316 South 1st Street, in Milwaukee, Wisconsin. The subject was armed with a handgun. The subject demanded phones to be placed into the bag he produced. The subject ordered them to hurry or he would shoot. After the phones were placed into the bag, the subject fled and was observed entering a blue hatchback sedan parked in front of the store. Over 20 devices were taken in the robbery. Sprint was a business involved in interstate commerce at the time of the robbery.

13. Based upon witnesses' descriptions and the recovered surveillance footage, the subject is described as a black male, approximately 230 pounds, heavy build, wearing a black ski mask, black hooded sweatshirt, gray jogging pants and gloves. The firearm, which was brandished during the robbery, was described as a black semi-automatic handgun.

14. Law enforcement collected video from the Sprint store and conducted a canvas in the area, which resulted in several surveillance videos being recovered and reviewed. These videos captured a blue Nissan Versa parked in the area before the robbery, from which the subject exited. After the robbery, the subject returned to the vehicle and put the black garbage bag in the trunk. The subject then drove away. The rear of the Versa had the make and model identifiers covered.

15. On October 29, 2019, at approximately 11:34 a.m., two masked subjects entered the T-Mobile store, located at 1528 South 108th Street, West Allis, Wisconsin. One subject was armed with a silver and black handgun. The victims were forced into a back room of the store and told to lie down. A store employee was told to open the safe containing cell phones and another

safe that contained cash. The phones were placed into black garbage bags. The cash, consisting of two $100 bills, two $50 bills, and rolls of quarters, was taken. The subjects then fled the store. T-Mobile was a business involved in interstate commerce at the time of the robbery.

16. Based upon witnesses' descriptions and the recovered surveillance footage, Subject #1 was described as a black male, possibly in his 30s, 5'8" to 5'9" tall, approximately 250 pounds, wearing a gray ski mask, dark navy blue puffy jacket, and gloves. Subject #2 was described as a black male, possibly in his 30s, approximately 6'0" tall, approximately 200 pounds, wearing a gray mask, dark clothing, and gloves. The firearm, which was brandished during the robbery, was described as a silver and black semi-automatic handgun.

17. Responding squads tracked the subject vehicle, identified as a blue Hyundai Elantra, which fled at a high rate of speed when officers attempted to stop the vehicle. As squads pursued the Elantra, it crashed in the alley in the 1300 block of South 37th Street, Milwaukee. Richard Tolbert exited the front passenger door and attempted to flee on foot but had a physical injury and was taken into custody. After a police perimeter was established and officers conducted a search of the area, Maurice Tolbert was taken into custody hiding in some foliage at the rear of 1313 South 35th Street. Law enforcement recovered the key fob to the Elantra where Maurice Tolbert was hiding.

18. The make and model emblems of the Elantra were covered with black electrical tape and a Wisconsin license plate, which was subsequently determined to have been reported as stolen, was attached over the Illinois plate registered to the Elantra, AZ-31096.

19. Along the flight path of the Elantra, officers recovered a loaded Taurus G2C 9mm silver and black handgun, bearing serial number TMD66339. This firearm had previously traveled in interstate commerce.

20. A Wisconsin State search warrant was executed on the Elantra. The items stolen from the T-Mobile were recovered in the trunk. Clothing, masks, and gloves consistent with the witnesses' descriptions and surveillance video in the T-Mobile robbery were located in the Elantra. Additionally, a black mask consistent with the masks worn in the October 2, 2019 and October 7, 2019 robberies was recovered from the Elantra. No personal cell phones were recovered.

21. A check of the Milwaukee County Criminal Justice Facility records for Maurice Tolbert reflected that A.P., 18XX West Wells, Milwaukee, WI, with phone number 414-865-3055 was listed as his emergency contact.

22. On November 1, 2019, at approximately 12:50 p.m., Maurice Tolbert called phone number 414-865-3055 from custody. During the recorded call, Maurice Tolbert identified the female as "Angel." He further provided her with the passcode to his phone, 329726, and information associated with his Apple ID (Grindfamily1@gmail.com, Lovelifeloyalty12). Based on that phone conversation, it was reasonable to assume that A.P. was in possession of Maurice Tolbert's phone and had access to Maurice Tolbert's stored iCloud information.

23. Based on my training and experience, I know that evidence of armed robberies is commonly found on the cellular phones belonging to the armed robber(s). This evidence often includes web-based searches for cellular telephone stores, contacts with individuals who purchased the stolen devices after the robberies, photographs of robbery proceeds or firearms used, price lists for the stolen phones, communication with co-conspirators, discussions related to, and the source of, any weapons used, and other similar evidence. In addition, I know that evidence found on cellular devices is commonly backed up, or stored, in "cloud" type services in the event a device is lost, stolen or damaged. As a result, law enforcement seeks access to Maurice Tolbert's stored iCloud information.

24. Records show that the recovered handgun, the Taurus G2C 9mm pistol bearing serial number TMD66339, was purchased by A.P. on October 6, 2019, the day before the October 7, 2019 Sprint robbery in which a consistent handgun was brandished. A.P. purchased the handgun at Dunham's Discount Sports, at 2550 South 108th Street, West Allis, WI. The purchase records reflect that A.P. provided her address as 11XX South Layton Blvd., Milwaukee, Wisconsin.

25. Maurice Tolbert is a convicted felon, and is therefore not lawfully allowed to purchase or possess a firearm himself.

26. On November 13, 2019, a Milwaukee Police Officer observed a gray Jeep Grand Cherokee with a REO Motors Dealer placard parked across the street from the apartment located at 508 North 28th Street. The Officer recorded the VIN on the vehicle as 1J4RR6GT8BC558075. A query of VIN 1J4RR6GT8BC558075 identified the registered owner as A.P., with listed address of 11XX South Layton Blvd., Milwaukee, Wisconsin, license plate AHC-6404.

27. On November 14, 2019, law enforcement conducted surveillance at 508 North 28th Street, Milwaukee, WI. At approximately 6:40 a.m., officers observed A.P. exit the apartment and brush snow off the gray Jeep Cherokee bearing REO Motors Dealer placard. A.P. returned to 508 North 28th Street and exited a few minutes later with two children. They entered the Grand Cherokee and departed.

28. On November 15, 2019, law enforcement officers executed a federal search warrant on the residence at 508 N. 28th Street, in Milwaukee. Various items of evidentiary value were recovered including, but not limited to, firearm boxes and records, ammunition, firearm magazines, cellular devices, and drug paraphernalia such as a "kilo press." Officers also recovered some of the clothing consistent with the clothing worn by one of the suspects in the October 2, 2019 robbery and the October 7, 2019 robbery.

29. Additionally, A.P. was interviewed regarding her knowledge of and involvement in the criminal violations being investigated. During this interview, A.P. explained that she had purchased multiple firearms for her boyfriend, Maurice Tolbert, who she knew to be a convicted felon. Ultimately, A.P. admitted to purchasing at least five firearms for Maurice Tolbert. A.P. explained that she does not know how firearms operate, and would never have purchased a firearm on her own because she felt she did not need to own firearms. Maurice Tolbert accompanied her to the gun stores, selected the firearms, and provided the cash to purchase the firearms on all but two (2) occasions. Maurice Tolbert then was the primary owner of the firearm. A.P. explained instances when Maurice Tolbert would return home and state he had been robbed and someone had stolen his firearm which would lead to her purchasing another firearm for him.

30. A.P. viewed still photos from the October 2, 2019 casing incident and robbery and the October 7, 2019 robbery. A.P. identified the suspect in the October 2, 2019 casing incident as someone who "favored" Richard Tolbert, although she had only seen Richard Tolbert on a couple of occasions. A.P. identified the firearm in the October 7, 2019 robbery as the firearm she purchased on October 6, 2019 from Dunham's for Maurice Tolbert.

31. During the interview with investigators, A.P. provided her telephone number as 414-865-3055 and provided Maurice Tolbert's telephone number as 312-978-8447.

32. Since A.P.'s interview, investigators have obtained firearms purchase records from several federal firearms dealers. In total, investigators have collected documents showing that A.P. has purchased at least six firearms since 2013. Those records reflect that on the following dates, A.P. purchased the following firearms:

a. January 6, 2013 – A.P. purchased one (1) firearm from Cabela's (FFL: 3-41-02642) located at 20200 Rogers Drive in Rogers, MN.

i. Manufacturer: North American Arms, Model: Mini, SN: E244884, Type: Revolver, Caliber: .22

b. December 1, 2017 – A.P. purchased one (1) firearm from Cabela's (FFL: 3-41-04460) located at 8400 Hudson Road, Woodbury, MN.

i. Manufacturer: Sccy Ind., Model: CPX-2, SN: 550661, Type: Pistol, Caliber: 9mm

c. March 11, 2019 – A.P. purchased one (1) firearm from Gander Outdoors (FFL: 3-31-09388) located at 6802 118th Avenue, Kenosha, WI.

i. Manufacturer: Taurus International, Model G2C, SN: TLO79819, Type: Pistol, Caliber: 9mm

d. April 11, 2019 – A.P. purchased one (1) firearm from Gander Outdoors (FFL: 3-31-09388) located at 6802 118th Avenue, Kenosha, WI.

i. Manufacturer: Glock, Model 26, SN: BGBS346, Type: Pistol, Caliber: 9mm

e. May 20, 2019 – A.P. purchased one (1) firearm from Gander Outdoors (FFL: 3-31-09388) located at 6802 118th Avenue, Kenosha, WI.

i. Manufacturer: Taurus International, Model G2C, SN: TMA80238, Type: Pistol, Caliber: 9mm

f. October 6, 2019 – A.P. purchased one (1) firearm from Dunham's (FFL: 3-39-17457) located at 2550 S. 108th Street, West Allis, WI.

i. Manufacturer: Taurus International, Model: G2C, SN: TMD66339, Type: Pistol, Caliber: 9mm

33. On November 19, 2019, SA Rutter reviewed publicly viewable portions of Facebook accounts and located Facebook profile with vanity name "Grind At Godspeed" (Facebook User ID 100014374597965).

34. SA Rutter located a Minnesota Department of Transportation (DOT) driver's license image (dated 4/23/18) of Maurice Tolbert and compared it to the publicly viewable images on the aforementioned Facebook page "Grind At Godspeed" – ID 100014374597965. The images appeared consistent and to represent the same individual.

35. During further review of the publicly viewable portion of the Facebook page "Grind At Godspeed" – ID 100014374597965, SA Rutter located multiple links to a YouTube music video titled "HE SAY SHE SAY MR.GRIND F/ AK OF DO OR DIE (OFFICIAL VIDEO)." This video was posted June 20, 2019 by "Mr. Grind." In the video, Maurice Tolbert is in possession of what appeared to be a small Glock-style handgun with an extended magazine. Below are two (2) screenshots from the aforementioned video.

36. The handgun shown in the video appears consistent with the Glock model 26 pistol purchased by A.P. on April 11, 2019. Additionally, three (3) Glock 9mm magazines were recovered during the aforementioned search warrant at 508 N. 28th Street in Milwaukee, WI on November 15, 2019.

37. A.P. also explained during her interview with investigators on November 15, 2019, that based upon Maurice Tolbert's instructions, she had erased the contents of Maurice Tolbert's iPhone and sold the phone. Affiant is aware that if an Apple iCloud user is logged into an Apple device, they must "sign out" of their account prior to the device being erased and reset to factory settings. Based on this information, it is reasonable to believe that Maurice Tolbert utilized Apple's iCloud services and that A.P. successfully erased his device using the information provided to her on November 1, 2019, by Maurice Tolbert. However, it is also reasonable to

believe that the information that was uploaded to Maurice Tolbert's Apple iCloud has not been affected by A.P.'s disposal of the contents of the device.

38. On November 19, 2019, SA Rutter sent a preservation request to Apple Inc., for the account grindfamily1@gmail.com.

39. There is probable cause to believe that evidence of Maurice Tolbert's violations of Title 18, United States Code, Sections 1951(a) (Hobbs Act robbery), 924(c) (use of a firearm during a crime of violence), and Title 18, United States Code, Section 922(g)(1) (felon in possession of a firearm) will be found on Maurice Tolbert's iCloud account

INFORMATION REGARDING APPLE ID AND ICLOUD[1]

65. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

66. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

67. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

68. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email

addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

69. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

70. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

71. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial

number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

72. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

73. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

74. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. For example, these communications and files may include, among other things, text messages or screen shots of text messages between Hatchett and his victims, records of Hatchett's posting of ads for prostitution, records of financial transactions of proceeds from Hatchett's sex trafficking crimes, and photographs evidencing his control, violence, and sex trafficking activities. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of the kind of criminal activity described herein, including to communicate and facilitate the offenses under investigation.

75. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

76. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

77. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators, or applications used to post ads for prostitution, conduct financial transactions with proceeds of sex trafficking, and/or make reservations for travel and hotels used for sex trafficking activities. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

78. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including, but not limited to, information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

79. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including

the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

80. Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID and iCloud account grindfamily1@gmail.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2011 to the present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account January 1, 2011 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All activity and transactional logs related to attempts to erase or restore the account or devices connected to the account to factory settings;

h. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

i. All records pertaining to the types of service used;

j. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

k. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **7 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1951(a) (Hobbs Act robbery), 924(c) (use of a firearm during a crime of violence), and Title 18, United States Code, Section 922(g)(1) (felon in possession of a firearm) involving Maurice Tolbert and his associates since December 1, 2017, to the Present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the location of such person(s) at a given time;

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

e. Evidence of illegal firearm possession;

f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

g. Evidence of communications between the subscriber and any co-conspirators; and

h. Evidence indicating how and where the subscriber spent and stored the fruits of his armed robberies.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [**PROVIDER**], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [**PROVIDER**]. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[PROVIDER]**, and they were made by **[PROVIDER]** as a regular practice; and

b. such records were generated by **[PROVIDER'S]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[PROVIDER]** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature